NextCard VISA Apply

Internet shopping as it should be.℠

Help/Faq

Security

When it comes to customer security, no one is more serious than NextCard Visa. We have designed one of the safest and most error-free systems around. To double check our security, we engaged PriceWaterhouseCoopers as independent security auditors to give us a clean bill of health. Our policy is to conduct regular third-party audits of our security to ensure that our standards never slip.

We'll walk you through our security, section by section, to let you know how we're protecting you. The NextCard Visa ensures that you are:

- Protected against somebody stealing your personal data
- Protected against electronic eavesdropping
- Protected against intercepted email
- Protected against hackers using your stolen credit card numbers
- Protected against failed security

Go Back

Protected against somebody stealing your personal data TOP

Your private account information is stored on an isolated NextCard Visa computer called a Customer Information Server. This server is carefully protected both physically and electronically.

Physically, the server is stored in a highly secure building maintained by Exodus Communications Inc., whose mission is to provide the highest degree of security for Internet applications. Key features of Exodus security:

- ***Fire Suppression System*** - State-of-the-art gas-based fire protection system, separate fire zones below the floor and above the ceiling, specialized heat/smoke sensors, and automatic local fire department notification
- ***Facility Security System*** - Motion sensors, secured access, video camera surveillance, security breach alarm, and 24 X 7 automatic local police department notification

- ***Personal Security System*** - 24 X 7 card key customer access to Internet Data Centers, monitoring, and 24 X 7 on-site personnel
- ***Server Cage*** - Our server is locked in a steel wire cage inside the secured Exodus building

Electronically, your private account information is NOT directly connected to the Internet. It sits behind a firewall. The firewall ensures that the sensitive information stored on the customer server is not available to unauthorized computers. It only allows certain messages from authorized computers through. The firewall we are using is a recognized industry standard, and exceeds the standards set by the International Computer Security Association (ICSA), a leading industry authority on the issue of Internet security.

Protected against electronic eavesdropping

TOP

You communicate with NextCard Visa through your computer's web browser. Your browser is a critical piece of our security infrastructure. We only support browsers that use Secure Sockets Layer (SSL) 3.0 or higher.

Your browser will handle these interactions automatically, so you do not have to take any extra steps to be protected. In fact, before you login or fill out an application, our server checks to make sure you're using one of the approved browsers.

SSL 3.0 provides protection against electronic eavesdropping through:

1. ***Server Authentication*** - Secure Sockets Layer 3.0 provides a way for you to verify that you are in fact logging on to the NextCard Visa server and not a site that is impersonating our server. Before you logon to NextCard Visa, our server sends NextCard Visa's public key to your browser program. SSL 3.0, lets you verify the identity of a server by viewing the site's Certificate. A Certificate is a way of associating a public key to a name. You can be sure that you are logged on to the NextCard Visa server by viewing our Certificate through your browser program when you're on the first page of the online application or login screen.
2. ***Data Encryption*** - Once SSL has authenticated the server, your browser and our server will establish a secret symmetric key. The symmetric key allows your browser and our server to exchange encrypted data. The symmetric key is valid for a single session only. If you log out and later come back to NextCard Visa, your browser and our server will negotiate a different symmetric key automatically. The symmetric key protects all of your communications with NextCard Visa.
3. ***Message Authentication Code*** - With data encryption in place, no outside party can understand our communications, but they

could still intercept a message and scramble it. To detect message tampering, SSL uses a message authentication code (MAC). A MAC is a piece of data that is computed, using pieces of the symmetric key and the message itself. Your browser always checks the MAC before interpreting a message from our server. If the message was scrambled by a hacker, the MAC would not correctly compute and your browser will alert you of possible security hazards. The chances of someone scrambling a message and then guessing the correct MAC are pretty slim: about 1 in 18,446,744,073,709,551,616 under 128-bit encryption.

Protected against intercepted email TOP

E-mail is a great way to pass messages, but it is not a secure communication channel. Here at NextCard Visa, all customer messages travel through SecureMail(sm), our secured, web-based communication system. Each of our customers has a personal SecureMail(sm) box that is easily accessible within our customer service website. And because SecureMail(sm) is entirely web-based, there's no need to learn a new email program or download additional software. SecureMail(sm) uses SSL 3.0 to protect all confidential communication.

Protected against hackers using your stolen credit card numbers TOP

In the wrong hands, technology has a way of distorting reality. For example, suppose you buy something with your NextCard Visa from an Internet merchant who turns out not to be a merchant, but a clever thief. The merchant website looked like a legitimate business and you took all the right precautions. But still, the hacker got your credit card number.

It is impossible to guarantee that an Internet thief will never get your NextCard Visa number, but we DO guarantee that you will not have to pay for any charges he rings up.

Here's our ***100% Safe Internet Shopping Pledge***[sm]: We will cover the full cost of any fraud against your account that arises from your usage of a NextCard Visa over the Internet. Shop online risk FREE and rest assured that you will not be held responsible for fraudulent charges to your NextCard Visa incurred by someone else.

Protected against failed security TOP

Technology moves forward at a rapid pace. The thieves get smarter, and so do the security systems. No matter what happens, you are always protected against security breaches with our ***100% Safe Internet Shopping Pledge***[sm].

Go Back